

L Number	Hits	Search Text	DB	Time stamp
-	21889	709/223-232,201-203,217-220.ccls.	USPAT; US-PGPUB; EPO; JPO	2004/08/26 09:43
-	7	709/223-232,201-203,217-220.ccls. and ((type near5 connection) same spoof\$3)	USPAT; US-PGPUB; EPO; JPO	2004/08/26 09:43


[Subscribe \(Full Service\)](#) [Register \(Limited Service, Free\)](#) [Login](#)

Search: The ACM Digital Library The Guide



THE ACM DIGITAL LIBRARY

[Feedback](#) [Report a problem](#) [Satisfaction survey](#)

 Terms used **type AND connection AND spoof**

 Found **38,289** of **141,680**

Sort results by

[Save results to a Binder](#)
[Try an Advanced Search](#)

Display results

[Search Tips](#)
[Try this search in The ACM Guide](#)
☐ Open results in a new window

Results 1 - 20 of 200

 Result page: [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#) [next](#)

Best 200 shown

 Relevance scale ☐ ☐ ☐ ☐ ☐

### 1 [Internet security attacks at the basic levels](#)

Marco de Vivo, Gabriela O. de Vivo, Germinal Isern

 April 1998 **ACM SIGOPS Operating Systems Review**, Volume 32 Issue 2

 Full text available: [pdf\(1.28 MB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#)

The Internet put the rest of the world at the reach of our computers. In the same way it also made our computers reachable by the rest of the world. Good news and bad news!. Over the last decade, the Internet has been subject to widespread security attacks. Besides the classical terms, new ones had to be found in order to designate a large collection of threats: *Worms, break-ins, hackers, crackers, hijacking, phrackers, spoofing, man-in-the-middle, password-sniffing, denial-of-service*, an ...

**Keywords:** Client-Server, Covert Channel, DNS, Denial of Service, Ethernet, Hijacking, ICMP, Kerberos, One-Time Password, Ping, RIP, Sniffing, Spoofing, TCP/IP

### 2 [DOS protection: Hop-count filtering: an effective defense against spoofed DDoS traffic](#)

Cheng Jin, Haining Wang, Kang G. Shin

 October 2003 **Proceedings of the 10th ACM conference on Computer and communication security**

 Full text available: [pdf\(213.86 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

IP spoofing has been exploited by Distributed Denial of Service (DDoS) attacks to (1) conceal flooding sources and localities in flooding traffic, and (2) coax legitimate hosts into becoming reflectors, redirecting and amplifying flooding traffic. Thus, the ability to filter spoofed IP packets near victims is essential to their own protection as well as to their avoidance of becoming involuntary DoS reflectors. Although an attacker can forge any field in the IP header, he or she cannot falsify t ...

**Keywords:** DDoS defense, TTL, host-based, networking, security

### 3 [Papers: Internet vulnerabilities related to TCP/IP and T/TCP](#)

Marco de Vivo, Gabriela O. de Vivo, Roberto Koeneke, Germinal Isern

 January 1999 **ACM SIGCOMM Computer Communication Review**, Volume 29 Issue 1

 Full text available: [pdf\(561.55 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#)

The Internet put the rest of the world at the reach of our computers. In the same way it also made our computers reachable by the rest of the world. Good news and bad news! Over the last decade, the Internet has been subject to widespread security attacks. Besides the classical terms, new ones had to be found in order to designate a large collection of


threats: *Worms, break-ins, hackers, crackers, hijacking, phrackers, spoofing, man-in-the-middle, password-sniffing, denial-of-service, and ...*

**Keywords:** Denial of Service, SYN Attack, Sniffing, Spoofing, T/TCP, TCP/IP

4 A requires/provides model for computer attacks

Steven J. Templeton, Karl Levitt

February 2001 **Proceedings of the 2000 workshop on New security paradigms**

Full text available:  [pdf\(704.16 KB\)](#) Additional Information: [full citation](#), [references](#), [citations](#), [index terms](#)

5 Managing routing tables for URL routers in content distribution networks

Zornitza Genova Prodanoff, Kenneth J. Christensen

May 2004 **International Journal of Network Management**, Volume 14 Issue 3


Full text available:  [pdf\(337.00 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

Large-scale content distribution networks (CDNs) can be built using URL routers to redirect client HTTP requests to the nearest content source. URL routers employ very large routing tables. To improve the manageability of CDNs, we propose to use URL signatures to reduce the size of routing tables and aggressive hashing to speed-up routing look-ups.

6 Encryption-based protection for interactive user/computer communication

Stephen Thomas Kent

September 1977 **Proceedings of the fifth symposium on Data communications**

Full text available:  [pdf\(846.33 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)

This paper develops a virtual connection model, complete with intruder, for interactive terminal-host communication and presents a set of protection goals that characterize the security that can be provided for a physically unsecured connection. Fundamental requirements for protocols that achieve these goals and the role of encryption in the design of such protocols are examined. Functional and security constraints on positioning of protection protocols in a communication system and the imp ...

7 Full papers: A taxonomy of DDoS attack and DDoS defense mechanisms

Jelena Mirkovic, Peter Reiher

April 2004 **ACM SIGCOMM Computer Communication Review**, Volume 34 Issue 2

Full text available:  [pdf\(209.38 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#)

Distributed denial-of-service (DDoS) is a rapidly growing problem. The multitude and variety of both the attacks and the defense approaches is overwhelming. This paper presents two taxonomies for classifying attacks and defenses, and thus provides researchers with a better understanding of the problem and the current solution space. The attack classification criteria was selected to highlight commonalities and important features of attack strategies, that define challenges and dictate the design ...

8 Formalizing the safety of Java, the Java virtual machine, and Java card

Pieter H. Hartel, Luc Moreau

December 2001 **ACM Computing Surveys (CSUR)**, Volume 33 Issue 4

Full text available:  [pdf\(442.66 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)

We review the existing literature on Java safety, emphasizing formal approaches, and the impact of Java safety on small footprint devices such as smartcards. The conclusion is that although a lot of good work has been done, a more concerted effort is needed to build a coherent set of machine-readable formal models of the whole of Java and its implementation. This is a formidable task but we believe it is essential to build trust in Java


safety, and thence to achieve ITSEC level 6 or Common Crite ...

**Keywords:** Common criteria, programming

9 A practical method to counteract denial of service attacks

Udaya Kiran Tupakula, Vijay Varadharajan

February 2003 **Proceedings of the twenty-sixth Australasian computer science conference on Conference in research and practice in information technology - Volume 16**

Full text available:  pdf(58.71 KB) Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)

Today distributed denial of service (DDoS) attacks are causing major problems to conduct online business over the Internet. Recently several schemes have been proposed on how to prevent some of these attacks, but they suffer from a range of problems, some of them being impractical and others not being effective against these attacks. In this paper, we propose a Controller-Agent model that would greatly minimize DDoS attacks on Internet. With a new packet marking technique and agent design our sc ...

**Keywords:** DoS, broad attack signatures, controller-agent model, denial of service, packet marking

10 On the effectiveness of route-based packet filtering for distributed DoS attack prevention in power-law internets

Kihong Park, Heejo Lee


August 2001 **ACM SIGCOMM Computer Communication Review , Proceedings of the 2001 conference on Applications, technologies, architectures, and protocols for computer communications**, Volume 31 Issue 4

Full text available:  pdf(313.26 KB) Additional Information: [full citation](#), [references](#), [citations](#), [index terms](#)

11 TCP-Peach: a new congestion control scheme for satellite IP networks

Ian F. Akyildiz, Giacomo Morabito, Sergio Palazzo

June 2001 **IEEE/ACM Transactions on Networking (TON)**, Volume 9 Issue 3

Full text available:  pdf(316.16 KB) Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)

Current TCP protocols have lower throughput performance in satellite networks mainly due to the effects of long propagation delays and high link error rates. In this paper, a new congestion control scheme called TCP-Peach is introduced for satellite networks. TCP-Peach is composed of two new algorithms, namely Sudden Start and Rapid Recovery, as well as the two traditional TCP algorithms, Congestion Avoidance and Fast Retransmit. The new algorithms are based on the novel concept of using d ...

**Keywords:** TCP protocols, congestion control, high bit error rates, long propagation delays, satellite networks

12 Disarming offense to facilitate defense

Danilo Bruschi, Emilia Rosti


February 2001 **Proceedings of the 2000 workshop on New security paradigms**

Full text available:  pdf(609.53 KB) Additional Information: [full citation](#), [references](#), [citations](#), [index terms](#)

**Keywords:** attack, computer and network security, defense, disarm, monitor, offense

**13** An architecture for secure wide-area service discovery

Todd D. Hodes, Steven E. Czerwinski, Ben Y. Zhao, Anthony D. Joseph, Randy H. Katz  
March 2002 **Wireless Networks**, Volume 8 Issue 2/3


Full text available:  pdf(365.68 KB) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

The widespread deployment of inexpensive communications technology, computational resources in the networking infrastructure, and network-enabled end devices poses an interesting problem for end users: how to locate a particular network service or device out of hundreds of thousands of accessible services and devices. This paper presents the architecture and implementation of a secure wide-area Service Discovery Service (SDS). Service providers use the SDS to advertise descriptions of available ...

**Keywords:** location services, name lookup, network protocols, service discovery

**14** Internet security standards: past, present, and future

Stephen Kent  
June 1994 **StandardView**, Volume 2 Issue 2

Full text available:  pdf(1.14 MB) Additional Information: [full citation](#), [references](#), [citations](#), [index terms](#)

**15** Using router stamping to identify the source of IP packets

Thomas W. Doepfner, Philip N. Klein, Andrew Koyfman  
November 2000 **Proceedings of the 7th ACM conference on Computer and communications security**

Full text available:  pdf(283.11 KB) Additional Information: [full citation](#), [references](#), [citations](#), [index terms](#)

**16** Topology discovery in heterogeneous IP networks: the NetInventory system

Yuri Breitbart, Minos Garofalakis, Ben Jai, Cliff Martin, Rajeev Rastogi, Avi Silberschatz  
June 2004 **IEEE/ACM Transactions on Networking (TON)**, Volume 12 Issue 3


Full text available:  pdf(435.97 KB) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)

Knowledge of the up-to-date physical topology of an IP network is crucial to a number of critical network management tasks, including reactive and proactive resource management, event correlation, and root-cause analysis. Given the dynamic nature of today's IP networks, keeping track of topology information manually is a daunting (if not impossible) task. Thus, effective algorithms for automatically discovering physical network topology are necessary. Earlier work has typically concentrated on e ...

**Keywords:** IP network management, SNMP MIBs, physical network topology, switched Ethernet

**17** Programming PHP with security in mind


Nuno Loureiro  
October 2002 **Linux Journal**, Volume 2002 Issue 102

Full text available:  html(15.73 KB) Additional Information: [full citation](#), [abstract](#), [index terms](#)

Can attackers subvert your web application? Not if you develop it with a healthy distrust of users.

**18** The session token protocol for forensics and traceback

Brian Carrier, Clay Shields  
August 2004 **ACM Transactions on Information and System Security (TISSEC)**, Volume 7 Issue 3

Full text available:  [pdf\(331.18 KB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [index terms](#)


In this paper we present the Session Token Protocol (STOP), a new protocol that can assist in the forensic analysis of a computer involved in malicious network activity. It has been designed to help automate the process of tracing attackers who log on to a series of hosts to hide their identity. STOP utilizes the Identification Protocol infrastructure, improving both its capabilities and user privacy. On request, the STOP protocol saves user-level and application-level data associated with a par ...

**Keywords:** Digital forensics, TCP traceback, auditing and intrusion detection, digital investigations, privacy

## 19 Multilink PPP

George E. Conant

September 1999 **Linux Journal**


Full text available:  [html\(21.14 KB\)](#) Additional Information: [full citation](#), [abstract](#), [index terms](#)

One Big Virtual WAN Pipe: MLPPP gives network managers the power to deliver WAN bandwidth on demand using an array of services

## 20 Industry track papers: Learning nonstationary models of normal network traffic for detecting novel attacks

Matthew V. Mahoney, Philip K. Chan

July 2002 **Proceedings of the eighth ACM SIGKDD international conference on Knowledge discovery and data mining**

Full text available:  [pdf\(1.12 MB\)](#) Additional Information: [full citation](#), [abstract](#), [references](#), [citations](#), [index terms](#)

Traditional intrusion detection systems (IDS) detect attacks by comparing current behavior to signatures of known attacks. One main drawback is the inability of detecting new attacks which do not have known signatures. In this paper we propose a learning algorithm that constructs models of normal behavior from attack-free network traffic. Behavior that deviates from the learned normal model signals possible novel attacks. Our IDS is unique in two respects. First, it is nonstationary, modeling pr ...

Results 1 - 20 of 200

Result page: [1](#) [2](#) [3](#) [4](#) [5](#) [6](#) [7](#) [8](#) [9](#) [10](#) [next](#)

The ACM Portal is published by the Association for Computing Machinery. Copyright © 2004 ACM, Inc.  
[Terms of Usage](#) [Privacy Policy](#) [Code of Ethics](#) [Contact Us](#)

Useful downloads:  [Adobe Acrobat](#)  [QuickTime](#)  [Windows Media Player](#)  [Real Player](#)

IEEE HOME | SEARCH IEEE | SHOP | WEB ACCOUNT | CONTACT IEEE



Membership Publications/Services Standards Conferences Careers/Jobs

**IEEE Xplore**  
 RELEASE 1.3

 Welcome  
 United States Patent and Trademark Office

 IEEE Xplore  
 1 Million Doc  
 1 Million User

[Help](#) | [FAQ](#) | [Terms](#) | [IEEE Peer Review](#)
[Quick Links](#)
» [Search Res](#)

## Welcome to IEEE Xplore®

- ☐ Home
- ☐ What Can I Access?
- ☐ Log-out

## Tables of Contents

- ☐ Journals & Magazines
- ☐ Conference Proceedings
- ☐ Standards

## Search:

- ☐ By Author
- ☐ Basic
- ☐ Advanced

## Member Services

- ☐ Join IEEE
- ☐ Establish IEEE Web Account
- ☐ Access the IEEE Member Digital Library

## IEEE Images

- ☐ Access the IEEE Enterprise File Cabinet

## Print Format

[Home](#) | [Log-out](#) | [Journals](#) | [Conference Proceedings](#) | [Standards](#) | [Search by Author](#) | [Basic Search](#) | [Advanced Search](#) | [Join IEEE](#) | [Web Account](#) | [New this week](#) | [OPAC Linking Information](#) | [Your Feedback](#) | [Technical Support](#) | [Email Alerting](#) | [No Robots Please](#) | [Release Notes](#) | [IEEE Online Publications](#) | [Help](#) | [FAQ](#) | [Terms](#) | [Back to Top](#)

 Your search matched **1** of **1064971** documents.

 A maximum of **500** results are displayed, **15** to a page, sorted by **Relevance** in **Descending** order.

## Refine This Search:

You may refine your search by editing the current search expression or entering a new one in the text box.


☐ Check to search within this result set

## Results Key:

**JNL** = Journal or Magazine    **CNF** = Conference    **STD** = Standard
1 **Agent-based distributed intrusion source identification**

Hongjun Wang; Ruijun Wang; Cuirong Wang; Yuan Gao;  
 Computer Networks and Mobile Computing, 2003. ICCNMC 2003. 2003  
 International Conference on , 20-23 Oct. 2003  
 Pages:341 - 344

[\[Abstract\]](#)    [\[PDF Full-Text \(2337 KB\)\]](#)    **IEEE CNF**


[Web](#) [Images](#) [Groups](#) [News](#) [Froogle](#) [more »](#)


[Advanced Search](#)  
[Preferences](#)

## Web

 Results 1 - 10 of about 38,400 for type connection spoof. (0.56 seconds)

### Spoofing a MAC Address to Reconnect to an ISP

... To **spoof** a MAC Address. ... that your ISP's installers used to establish Internet **connection** to the router. ... Then, in step 6, **type** Use This MAC Address, entering the ...

kbserver.netgear.com/kb\_web\_files/n101227.asp - 24k - [Cached](#) - [Similar pages](#)

### [PDF] Spoof Bounce

File Format: PDF/Adobe Acrobat - [View as HTML](#)

... Stopping and detecting **spoof** bounce attacks ... Another indication that this **type** of attack might be going ... a higher than normal number of **connection** requests that ...

www.giac.org/practical/gsec/Kevin\_Dixon\_GSEC.pdf - [Similar pages](#)

### Here's what you need to run Spoofer:

... the sequence numbers during the **spoof** to get ... To run, **type**: "Spoofer trusted\_hostname target\_host dead\_host ... that will not respond to TCP **connection** setup packets ...

www.tisl.ukans.edu/~jkeimig/spoof/frames/main.html - 14k - [Cached](#) - [Similar pages](#)

### The Whole-Web Spoofing Attack

... you naturally assume that you should **type** the name ... victim's browser shows the secure-**connection** icon (usually ... is difficult for the attacker to **spoof** the entire ...

bau2.uibk.ac.at/matic/spoofing.htm - 25k - [Cached](#) - [Similar pages](#)

### What is spoof? - A Word Definition From the Webopedia Computer ...

... WAN **connections** incur fees only when they are transmitting data. To reduce this problem, routers and other network devices can be programmed to **spoof** replies ...

www.webopedia.com/TERM/S/spoof.html - 38k - [Cached](#) - [Similar pages](#)

### Free Fake Email, Anonymous Email

... You can **spoof** any email address and send it to anyone you like. Sign Up. How to Send Fake Mail Using SMTP Servers? ... This **type connection** is untraceable. ...

anonmail.topcities.com/sendfakemail.html - 20k - [Cached](#) - [Similar pages](#)

### : Re: secure replacements for passwords

... If someone attempts to **spoof** the **connection**, they can do ... replacing it to the other side of the **connection**. Hopefully, this **type** of spoofing can be prevented by ...

www.mice.cs.ucl.ac.uk/multimedia/misc/tcp\_ip/8702.mm.www/0066.html - 7k - [Cached](#) - [Similar pages](#)

### Hack In The Box :: View topic - Remotely Connecting to An ip

... to that port, you should be able to **connect** to it ... simple UserAgent check), but you can easily **spoof** that info ... There can also be 'deep level' **type** of protection ...

https://forum.hackinthebox.org/viewtopic.php?p=50099 - 53k - [Cached](#) - [Similar pages](#)

### War Tools! Scan, Sniff, Spoof and Hijack 2

... Scan, Sniff, **Spoof** and Hijack \_\_\_\_ Note ... on a Unix **type** computer - as ... is going on with each **connection**. ...

www.secinf.net/harmless\_hacking\_book/War\_Tools\_Scan\_Sniff\_Spoof\_and\_Hijack\_2.html - 57k - [Cached](#) - [Similar pages](#)

### Prelude Hybrid IDS: [3514] (changeset) - Trac

... medium; \ assessment.impact.completion=failed; \ assessment.impact.**type**=recon; \ assessment ... PIX-1-106022: Deny protocol **connection spoof** from source\_address to ...

trac.prelude-ids.org/trac.cgi/changeset/3514 - 14k - [Cached](#) - [Similar pages](#)